UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE TJX COMPANIES RETAIL SECURITY BREACH LITIGATION THIS DOCUMENT RELATES TO: FINANCIAL INSTITUTIONS TRACK	Master Docket No. 07-10162-WGY
MASSACHUSETTS BANKERS ASSOCIATION; CONNECTICUT BANKERS ASSOCIATION; MAINE ASSOCIATION OF COMMUNITY BANKS; EAGLE BANK; SAUGUSBANK; COLLINSVILLE SAVINGS SOCIETY; and AMERIFIRST BANK, Individually and on behalf of a class of all similarly situated financial institutions Plaintiffs v. THE TJX COMPANIES, INC. Defendant	JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

The Massachusetts Bankers Association, the Connecticut Bankers Association, and the Maine Association of Community Banks (collectively, the "Bankers Associations"), and Eagle Bank, Saugusbank, Collinsville Savings Society, and AmeriFirst Bank (collectively, the "Banks") (the Bankers Associations and the Banks are referred to herein as the "Plaintiffs"), individually and on behalf of a class of all similarly

situated financial institutions, assert the following in their Complaint against The TJX Companies, Inc. ("TJX" or "Defendant"):

Summary of Action

1. In the largest data security breach ever to have occurred in the United States, at least 45.7 million credit cards and debit cards were compromised because of TJX's acts and omissions. Plaintiffs bring this class action on their own behalf and on behalf of all similarly situated financial institutions seeking redress and damages caused by TJX's misrepresentations, unfair and deceptive acts and practices, negligence, breach of contract, and improper retention of certain customer confidential information in connection with that data security breach. TJX's failure to adequately safeguard customer confidential information and related data and TJX's failure to maintain adequate encryption, intrusion detection and prevention procedures in its computer systems caused the losses hereinafter set forth.

2. As a result of TJX's wrongful actions, customer information was accessed from TJX's computer systems. As a result, class member financial institutions have incurred significant losses associated with credit and debit card reissuance, customer reimbursement for fraud losses, lost interest and transaction fees (including lost interchange fees), lost customers, administrative expenses associated with monitoring and preventing fraud and administrative expenses in dealing with customer confusion, fraud claims and card reissuance.

3. Plaintiffs seek to recover damages caused by Defendant's negligent misrepresentations, unfair and/or deceptive acts or practices in Massachusetts in violation of Mass. Gen. Laws c. 93A, §§ 2, 11, negligence, and breach of contract.

4. Plaintiffs also seek a finding and injunctive relief enjoining Defendant from improperly retaining customer data.

Jurisdiction and Venue

5. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), in that (1) the Class (as defined below) has more than 100 hundred Class members, (2) the amount at issue exceeds five million dollars ($5,000,000.00), exclusive of interest and costs, and (3) minimal diversity exists as at least one plaintiff and one defendant are citizens of different states.

6. Defendant is subject to the provisions of Mass. Gen. Laws c. 93A, § 11 in that the unfair or deceptive acts or practices complained of occurred primarily and substantially within the Commonwealth of Massachusetts.

7. Venue in the United States District Court for the District of Massachusetts is appropriate, pursuant to 28 U.S.C. § 1391(a), in that Defendant resides in the District of Massachusetts and a substantial part of the events or omissions giving rise to the claim occurred in the District of Massachusetts.

Parties

A. Representative Plaintiffs

8. The Massachusetts Bankers Association is a non-stock corporation acting as a banking trade association with its principal place of business located in Boston, Massachusetts.

9. The Massachusetts Bankers Association represents more than 200 banks all across Massachusetts and New England.

10. The stated purpose of the Massachusetts Bankers Association is to promote the general welfare and usefulness of banks and banking institutions; to secure uniformity of action, together with the practical benefit derived from the discussion of subjects of importance to the banking, commercial and industrial interests of the State of Massachusetts, and especially in order to secure the proper consideration of questions regarding the financial and commercial usages, customs and laws which affect the banking interests of the State of Massachusetts, and for the protection against loss by crime.

11. The Connecticut Bankers Association is a non-stock Connecticut corporation acting as a banking trade association with its principal place of business located in Farmington, Connecticut.

12. The Connecticut Bankers Association represents more than 60 banks conducting business in Connecticut.

13. The stated purpose of the Connecticut Bankers Association is to represent financial institutions in the State of Connecticut and to serve as the voice of its members in matters of their common interest.

14. The Maine Association of Community Banks is a non-profit banking trade association with its principal place of business located in Portland, Maine.

15. The Maine Association of Community Banks represents more than 20 banks all across Maine.

16. The stated purpose of the Maine Association of Community Banks is to represent community-oriented banks in the State of Maine.

17. The Bankers Associations collectively represent approximately three hundred banks in New England.

18. Eagle Bank is a state-chartered mutual savings bank with its principal place of business located in Everett, Massachusetts.

19. Eagle Bank issued MasterCard debit cards to its customers.

20. Saugusbank is a state-chartered mutual co-operative bank with its principal place of business located in Saugus, Massachusetts.

21. Saugusbank issued Visa debit cards to its customers.

22. Collinsville Savings Society is a state-chartered mutual savings bank with its principal place of business located in Collinsville, Connecticut.

23. Collinsville Savings Society issued MasterCard debit cards to its customers.

24. AmeriFirst Bank is a retail bank with its principal place of business located in Union Springs, Alabama.

25. AmeriFirst Bank issued MasterCard debit cards to its customers.

B. Defendant

26. Defendant TJX is a Delaware corporation with its principal place of business located in Framingham, Massachusetts. TJX's operating segments or divisions in the United States include, inter alia, Marshalls and T.J. Maxx, referred to as MarMaxx, Home Goods, A.J. Wright and Bob's Stores.

27. T.J. Maxx is the largest off price retail chain in the United States with 821 stores including 47 in Massachusetts and 25 in Connecticut. Marshalls is the second

largest off price retail chain in the United States with 734 stores including 48 in Massachusetts and 23 in Connecticut.

Class Action Allegations

28. Plaintiffs bring this action on their own and on behalf of all other financial institutions similarly situated for the purpose of asserting claims alleged herein on a common basis, pursuant to 28 U.S.C. § 1332(d). The proposed Class (the "Class") is defined as:

> Financial institutions that have suffered damages and/or harm as a result of data breaches set forth herein with respect to personal and financial information of customers who used debit or credit cards at TJX's retail stores.

29. The named representative Plaintiff Banks are members of the Class they seek to represent.

30. The named representative Plaintiff Bankers Associations seek to protect the interests of their members in preventing unfair or deceptive practices by large retail merchants including improper retention of customer data and inadequate data security procedures. These interests are directly related to the Bankers Associations' purpose, and the Bankers Associations have been and continue to represent their member banks in advancing data security and protection policies at the state and federal level and with Mastercard and Visa.

31. This action is brought and may be properly maintained as a class action pursuant to 28 U.S.C. § 1332(d) . This action satisfies the procedural requirements set forth by Fed. R. Civ. P. 23.

32. The conduct of Defendant has caused injury to members of the proposed Class. The proposed Class is so numerous that joinder of all members is impracticable.

33. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b. Whether Defendant negligently misrepresented that it did not retain customer financial information and negligently represented that it provided security as to its computer systems to prevent intrusions.

c. Whether conduct (action or inaction) of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

d. Whether Defendant knew or should have known of the vulnerability of its computer systems to breach;

e. Whether Defendant knew or should have known of the risks to financial institutions inherent in failing to protect such financial and personal information;

f. Whether Defendant improperly retained customer personal and financial information despite representations that it would not keep such information;

g. Whether Defendant disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of customers;

h. Whether Defendant engaged in unfair and deceptive acts or practices by utilizing and maintaining a computer system for customer purchases and returns that did not adequately protect customer information, in violation of Mass. Gen. Laws c. 93A, §§ 2, 11 which prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce . . ."

i. Whether Defendant engaged in unfair and deceptive acts or practices by disregarding industry standards and its own representations regarding the protection of customer financial and personal information, in violation of Mass. Gen. Laws c. 93A, §§ 2, 11;

j. Whether Defendant engaged in unfair and deceptive acts or practices by retaining customers' financial and personal information beyond the proper period of time, in violation of Mass. Gen. Laws c. 93A, §§ 2, 11;

k. Whether Plaintiffs and members of the proposed Class have been injured by Defendant's negligent misrepresentations, violations of Mass. Gen. Laws c. 93A, §§ 2, 11, negligence, and breach of contract;

l. Whether Plaintiffs and members of the proposed Class have been damaged by the conduct of Defendant;

m. Whether Defendant's violations of Mass. Gen. Laws c. 93A, §§ 2, 11 were knowing, willful, wanton, intentional, deliberate and/or malicious or otherwise caused proximate damages to the Plaintiffs such that Class members are entitled to an award of multiple or punitive damages and attorneys fees;

n. Whether Defendant breached its duties to exercise reasonable and due care in obtaining, using, retaining and safeguarding the personal and financial information of bank customers; and

o. Whether Defendant breached its obligations to Plaintiffs and Class members as third party beneficiaries of Defendant's contract with Fifth Third Bank.

34. The claims of the representative Plaintiffs are typical of the proposed Class. The same events and conduct that give rise to Plaintiffs' claims and legal theories also give rise to the claims and legal theories of the proposed Class. The Bankers Associations' claims are representative of the claims of financial institutions that are members of the proposed Class.

35. The representative Plaintiffs will fairly and adequately represent the interests of the proposed Class. There are no disabling conflicts of interest between the representative Plaintiffs and the proposed Class.

36. The named representatives are part of the proposed Class, possess the same interests, and suffer the same injuries as Class members, making their interests

coextensive with those of the Class. The interests of the representative Plaintiffs and members of the proposed Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

37. Common questions of law and fact predominate over individualized questions. A Class action is superior to other methods for the fair and efficient adjudication of this controversy.

38. Plaintiffs are represented by experienced counsel who are qualified to handle this case. The lawsuit will be capably and vigorously pursued by the representative Plaintiffs and their counsel.

Factual Background

39. TJX purports to be the leading off-price apparel and home fashion retailer in the United States and worldwide, with $16 billion in revenues in 2005. Its stock trades on the New York Stock Exchange under the symbol TJX.

40. TJX operates more than 2,400 retail stores under such chains as T.J. Maxx, Marshalls, HomeGoods, A.J. Wright and Bob's Stores. Of these stores, 146 are located in Massachusetts, 76 are located in Connecticut and 13 are located in Maine.

41. On January 17, 2007, TJX first publicly announced that it had experienced a wide-reaching security breach that may leave millions of its customers around the world exposed to fraud and identity theft from transactions that date back to 2003. TJX's press release stated, in relevant part:

> The TJX Companies, Inc. (NYSE:TJX) today announced that it has suffered an unauthorized intrusion into its computer systems that process and store information related to customer transactions. While TJX has specifically identified some customer information that has been stolen

> from its systems, the full extent of the theft and affected customers is not yet known. This intrusion involves the portion of TJX's computer network that handles credit card, debit card, check, and merchandise return transactions for customers of its T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico, and its Winners and HomeSense stores in Canada, and may involve customers of its T.K. Maxx stores in the U.K. and Ireland. The intrusion could also extend to TJX's Bob's Stores in the U.S.

42. Through its investigation, TJX claimed to have learned the following with respect to the intrusion:

- Portions of the information stored in the affected part of TJX's network regarding credit and debit card sales transactions in TJX's stores (excluding Bob's Stores) in the U.S., Canada, and Puerto Rico during 2003, as well as such information for these stores from the period from mid-May through December, 2006 may have been accessed in the intrusion.

- TJX does not know if it will be able to identify additional information of specific customers that may have been taken.

43. TJX's press release also stated that TJX discovered the intrusion in "mid-December, 2006." Nevertheless, TJX did not announce the intrusion until approximately one month later, when it issued its January 17, 2007 press release.

44. TJX's press release further noted that after the security breach occurred, TJX "significantly strengthened the security of its computer systems." TJX has not publicly stated the nature of the insufficiencies that required strengthening.

45. On its website, in a section titled "Frequently Asked Questions" concerning the security breach, TJX alluded to the possibility that some customers' drivers' license numbers may be the same as their social security numbers.

46. On January 19, 2007, The Wall Street Journal reported that the security breach "exposed millions of consumers to potential fraud." It reiterated that the number

of exposed cards could exceed 40 million, citing representatives from Visa. The article also stated that "patterns of counterfeit fraud have been reported on some of the affected accounts,'" quoting a letter from Visa.

47. The January 19, 2007 Wall Street Journal article also stated that U.S. retailers including TJX are required to follow "stringent card-industry rules," which "require merchants to validate a series of security measures, such as the establishment of firewalls to protect databases." The article also noted that merchants are prohibited from storing unprotected cardholder information.

48. On January 25, 2007, The Wall Street Journal reported that fraudulent purchases using credit and debit card numbers stolen from TJX had already surfaced in several states. Prior to and during the months of January and February 2007, Plaintiffs were directly damaged by actual fraud losses and reimbursement of customer transactions. Hundreds of thousands of customer accounts have been affected in this manner.

49. In its Form 10-K for the fiscal year ended January 27, 2007, TJX provided further details on the security breach. Specifically, TJX reported in pertinent part as follows:

> On February 18, 2007, in the course of our ongoing investigation, we found evidence that the Computer Intrusion may have been initiated earlier than previously reported and that additional customer information potentially had been stolen. On February 21, 2007, we publicly announced additional findings on the timing and scope of the Computer Intrusion.
>
> *Timing of Computer Intrusion.* Based on our investigation to date, we believe that our computer systems were first accessed by an unauthorized Intruder in July 2005, on subsequent dates in 2005 and from mid-May 2006 to mid-January 2007, but that no customer data were stolen after December 18, 2006....

> *Systems Affected in the Computer Intrusion.* We believe that information was stolen in the Computer Intrusion from a portion of our computer systems in Framingham, MA that processes and stores information related to payment card, check and unreceipted merchandise return transactions for customers of our T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico and our Winners and HomeSense stores in Canada ("Framingham system")....
>
> We have sought to identify customer information stolen in the Computer Intrusion. To date, we have been able to identify only some of the information that we believe was stolen. Prior to discovery of the Computer Intrusion, we deleted in the ordinary course of business the contents of many files that we now believe were stolen. In addition, the technology used by the Intruder has, to date, made it impossible for us to determine the contents of most of the files we believe were stolen in 2006. Given the scale and geographic scope of our business and computer systems and the time frames involved in the Computer Intrusion, our investigation has required a substantial period of time to date and is not completed. We are continuing to try to identify information stolen in the Computer Intrusion through our investigation, but, other than the information provided below, we believe that we may never be able to identify much of the information believed stolen.

50. In the same filing, TJX also provided further details about what data it believed had been stolen. In this regard, TJX stated that "We suspect that the data believed stolen in 2005 related to somewhere between approximately half to substantially all of the transactions at U.S., Puerto Rican and Canadian stores during the period from December 31, 2002 through June 28, 2004." In addition, TJX stated that the files "stolen in 2006 could have included the data that we believe were stolen in 2005, as well as other data relative to some customer transactions from December 31, 2002 through mid-May 2006."

51. Significantly, TJX admitted that much of the data stolen was not encrypted, stating that "the technology utilized in the Computer Intrusion during 2006 could have enabled the Intruder to steal payment card data from our Framingham system during the payment card issuer's approval process, in which

data ... is transmitted to payment card issuer's without encryption." TJX further stated that "we believe that the Intruder had access to the decryption tool for the encryption software utilized by TJX."

52. Most recently, in a May 4, 2007 article, the *Wall Street Journal* reported that investigators now believe that the security breach began during the summer of 2005. As reported by the article:

> The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn.
>
> There, investigators now believe, hackers pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into the central database of Marshalls' parent, TJX Cos. in Framingham, Mass., to repeatedly purloin information about customers.
>
> The $17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company -- which also owns T.J. Maxx, Home Goods and A.J. Wright -- had no idea what was going on. The hackers, who have not been found, downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's internal investigation says they may have grabbed as many as 200 million card numbers all told from four years' records.
>
> When wireless data networks exploded in popularity starting around 2000, the data was largely shielded by a flawed encoding system called Wired Equivalent Privacy, or WEP, that was quickly pierced. The danger became evident as soon as 2001, when security experts issued warnings that they were able to crack the encryption systems of several major retailers.
>
> By 2003, the wireless industry was offering a more secure system called Wi-Fi Protected Access or WPA, with more complex encryption. Many merchants beefed up their security, but others including TJX were slower to make the change. An auditor later found the company also failed to install firewalls and data encryption on many of its computers using the wireless network, and didn't properly install another layer of security software it had bought. The company declined to comment on its security measures.

The hackers in Minnesota took advantage starting in July 2005. Though their identities aren't known, their operation has the hallmarks of gangs made up of Romanian hackers and members of Russian organized crime groups that also are suspected in at least two other U.S. cases over the past two years, security experts say. Investigators say these gangs are known for scoping out the least secure targets and being methodical in their intrusions, in contrast with hacker groups known in the trade as "Bonnie and Clydes" who often enter and exit quickly and clumsily, sometimes strewing clues behind them.

The TJX hackers did leave some electronic footprints that show most of their break-ins were done during peak sales periods to capture lots of data, according to investigators. They first tapped into data transmitted by hand-held equipment that stores use to communicate price markdowns and to manage inventory. "It was as easy as breaking into a house through a side window that was wide open," according to one person familiar with TJX's internal probe. The devices communicate with computers in store cash registers as well as routers that transmit certain housekeeping data.

After they used that data to crack the encryption code the hackers digitally eavesdropped on employees logging into TJX's central database in Framingham and stole one or more user names and passwords, investigators believe. With that information, they set up their own accounts in the TJX system and collected transaction data including credit-card numbers into about 100 large files for their own access. They were able to go into the TJX system remotely from any computer on the Internet, probers say....

They were so confident of being undetected that they left encrypted messages to each other on the company's network, to tell one another which files had already been copied and avoid duplicating work. The company says the hackers may even have lifted bank-card information as customers making purchases waited for their transactions to be approved. TJX transmitted that data to banks "without encryption," it acknowledged in an SEC filing. That violates credit-card company guidelines, experts say.

While the hackers were stealing the data, they were selling it on the Internet on password-protected sites used by gangs who then run up charges using fake cards printed with the numbers, investigators say....

As the stolen TJX numbers were being used in Florida, the company was getting a stern warning about its poor security from a routine audit. The auditor told the company last Sept. 29 that it wasn't complying with many of the requirements imposed by Visa and MasterCard, according to a

person familiar with the report. The auditor's report cited the outmoded WEP encryption and missing software patches and firewalls.

53. Visa U.S.A. ("Visa") is a privately held membership corporation organized under Delaware law that supports Visa credit and debit cards issued by financial institutions ("Issuing Banks") to consumers and processes transactions made with those cards on behalf of financial institutions ("Acquiring Banks") that acquire the card-paid transactions of a merchant enrolled in Visa's program ("Visa Merchant").

54. MasterCard Inc. ("MasterCard") is a publicly traded Delaware corporation that supports MasterCard credit and debit cards issued by financial institutions ("Issuing Banks") to consumers and processes transactions made with those cards on behalf of financial institutions ("Acquiring Banks") that acquire the card-paid transactions of a merchant enrolled in MasterCard's program ("MasterCard Merchant").

55. Plaintiff Banks serve as Issuing Banks, which issue debit cards to their customers.

56. TJX, a seller of retail goods, is a Visa and MasterCard Merchant and accepts Visa and MasterCard card transactions from consumers.

57. Fifth Third Bank ("Fifth Third") is a bank with its principal place of business in Cincinnati, Ohio.

58. Fifth Third serves as an Acquiring Bank, processing Visa and MasterCard transactions on behalf of TJX.

59. TJX, Fifth Third, Issuing Banks, Visa, and MasterCard together participate in systems whereby consumers may purchase goods from TJX retail stores using their Visa and MasterCard cards (the "Visa and MasterCard Systems").

60. Visa issues "Visa U.S.A. Operating Regulations" ("Visa Operating Regulations"). MasterCard issues regulations that are contained in "MasterCard International Bylaws and Rules", "MasterCard International Security Rules and Procedures", "MasterCard International Authorization System Manual", "MasterCard International Payment Card Industry Data Security Standard", and "MasterCard International Operating Regulations" ("MasterCard Operating Regulations"). The Visa Operating Regulations and the MasterCard Operating Regulations are hereinafter collectively referred to as "Card Operating Regulations".

61. The Card Operating Regulations governed the conduct of TJX at all times relevant to this action.

62. Fifth Third has a contract with Visa and a contract with MasterCard that requires Fifth Third to comply with the Card Operating Regulations.

63. TJX has a contract with Fifth Third that requires TJX to comply with the Card Operating Regulations.

64. TJX is required to comply with the Card Operating Regulations, including those portions of the Card Operating Regulations that mandate safeguarding of cardholder information and that prohibit retention or storage of Visa and MasterCard cardholder account numbers, personal information, magnetic stripe information, or Visa and MasterCard transaction information subsequent to the card authorization.

65. For example, Visa, in a section of its website entitled Visa USA *Cardholder Information Security Program* (CISP) – *An Overview*, states "To achieve CISP compliance, all Members, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to

safeguarding sensitive data for all card brands." Visa further states that "Acquirers are responsible for ensuring that all of their merchants comply with the PCI Data Security Standard requirements."

See http://usa.visa.com/merchants/risk_management/cisp_merchants.html.

66. Similarly, MasterCard states on its website, "A key focus of [MasterCard's security program]...is to ensure that Merchants and Service Providers are securely storing MasterCard account data in accordance with the Payment Card Industry Data Security Standard (PCI Data Security Standard)." *See* http://www.mastercard.com/us/sdp/index.html.

67. The PCI Standards require the following:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know

- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

68. At all times relevant hereto, TJX knew or should have known that the Card Operating Regulations forbid it from retaining or storing Visa and MasterCard card magnetic stripe information subsequent to the authorization of a transaction.

69. At all times relevant hereto, TJX knew or should have known that the Card Operating Regulations forbid it from disclosing any Visa or MasterCard cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the Acquiring Bank, or the Acquiring Bank's agents.

70. At all times relevant hereto, TJX knew or should have known that the Card Operating Regulations require it to secure and keep confidential Visa and MasterCard cardholder information and magnetic stripe information from unauthorized disclosure, as set out in the Card Operating Regulations.

71. TJX's contract with Fifth Third and its involvement in this complex web of interrelated financial institutions required that TJX: (a) comply with the Card Operating Regulations; (b) properly secure Visa and MasterCard card magnetic stripe

information; (c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

72. TJX, at all times relevant to this action, represented and had a duty to Plaintiff Banks to: (a) comply with the Card Operating Regulations; (b) properly secure Visa and MasterCard card magnetic stripe information; (c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

73. TJX negligently allowed Visa and MasterCard card magnetic stripe information to be compromised.

74. TJX negligently utilized a computer system that retained, stored and/or disclosed (or allowed to be disclosed) Visa and MasterCard card magnetic stripe information.

75. The Visa and MasterCard cards from which TJX retained magnetic stripe information included millions of Visa and MasterCard cards issued by Issuing Banks to their customers. A substantial number of Issuing Banks' customers used the Visa and MasterCard cards at TJX's stores and those transactions enabled TJX to retain and store information from those Visa and MasterCard cardholders through the magnetic stripe on the Visa and MasterCard cards.

76. Data from the magnetic stripe on millions of Visa and MasterCard cards, issued by banks to their customers and used by those customers at TJX stores, was accessed from TJX.

77. Third parties were able to access, obtain and use the Visa and MasterCard card magnetic stripe information obtained to fraudulently make transactions and to sell, transfer, use or attempt to use such information for fraudulent purposes.

78. In accordance with its operating procedures, Visa notifies Issuing Banks of security breaches impacting Visa issued debit and credit cards through a system of alerts, known as Compromised Account Management System Alerts or "CAMS Alerts." CAMS Alerts: (1) identify generally the type of information compromised; (2) identify the timeframe such information was compromised; and (3) provide the Issuing Banks with a list of card numbers that it has issued that have been exposed to fraud risk.

79. In accordance with its operating procedures, MasterCard notifies Issuing Banks of security breaches impacting MasterCard issued debit and credit cards through a Security Alert.

80. As indicated by news reports, the Visa CAMS Alerts and the MasterCard Security Alerts, TJX retained magnetic stripe information from millions of Visa and MasterCard cards issued by Plaintiff Banks to their customers. A substantial number of Plaintiff Banks' customers used the Visa and MasterCard cards at TJX stores and those transactions enabled TJX to retain and store information from those Visa and MasterCard cardholders through the magnetic stripe on the Visa and MasterCard cards.

81. As a result of the events set forth in paragraphs 1 through 80 of this Complaint, Plaintiff Banks and members of the proposed Class, to protect their customers and avoid fraud losses, cancelled Visa and MasterCard cards they had issued. Plaintiff Banks and members of the proposed Class reissued cards with new account numbers and magnetic stripe information to customers.

82. The cancellation and reissuance of cards resulted in damages and losses to Plaintiff Banks and members of the proposed Class of up to $25 per card.

83. As a result of the events set forth in paragraphs 1 through 80 of this Complaint, Plaintiff Banks and members of the proposed Class suffered losses related to reimbursement of fraudulent charges or reversal of customer charges.

84. Plaintiff Banks and members of the proposed Class suffered losses related to lost interest and transaction fees (including lost interchange fees).

85. Plaintiff Banks and members of the proposed Class suffered losses related to administrative expenses and overhead charges associated with monitoring and preventing fraud.

86 Plaintiff Banks and members of the proposed Class suffered losses related to administrative expenses associated with addressing customer confusion and fraud claims.

87. Plaintiff Banks and members of the proposed Class have incurred additional costs, expenses, and other consequential damages, including, but not limited to, potential damages to Plaintiff Banks' reputations and lost customers.

88. Plaintiff Banks and members of the proposed Class will suffer additional monetary harm for the costs and expenses described above as additional fraud alerts and fraud charges are discovered and occur.

COUNT ONE
NEGLIGENT MISREPRESENTATION

89. Plaintiffs incorporate paragraphs 1 through 88 of this Complaint by reference herein.

90. In participating in the Visa and MasterCard Systems, TJX falsely represented that it would comply with the Card Operating Regulations and would safeguard customer data in order to induce banks to act as Issuing Banks and provide their customers with Visa and MasterCard cards for use at TJX stores.

91. TJX's compliance with the Card Operating Regulations and safeguarding of customer data were material facts upon which the Plaintiff Banks (the Issuing Banks) relied.

92. TJX, which knew or should have known that it was not in compliance with the Card Operating Regulations and was not safeguarding customer data, represented that it was so doing, which included a representation that it would not retain, store or disclose the magnetic stripe information and would maintain the confidentiality of the information.

93. Plaintiff Banks agreed to act as the Issuing Banks for Visa and MasterCard card transactions expecting that large retail chains such as TJX would comply with the Card Operating Regulations and would safeguard customer data. Plaintiff Banks relied upon and acted in reliance on such representations by TJX.

94. Plaintiff Banks would have attempted to take additional steps to protect themselves but for the misrepresentations of TJX as set forth above.

95. TJX failed to exercise reasonable care in obtaining and in communicating the information that Plaintiff Banks relied upon.

96. Plaintiff Banks justifiably relied upon the false representations made by TJX regarding the security and confidentiality of the Visa and MasterCard card information.

97. Plaintiffs and members of the proposed Class have suffered damages as set forth above as a result of TJX's misrepresentations.

COUNT TWO
UNLAWFUL DECEPTIVE ACTS AND PRACTICES UNDER M.G.L. CHAPTER 93A, SECTION 11

98. Plaintiffs incorporate paragraphs 1 through 97 of this Complaint by reference herein.

99. TJX is a Delaware corporation headquartered in Massachusetts that is engaged in trade or commerce in the Commonwealth of Massachusetts.

100. The TJX computer systems that process and store information related to credit and debit card transactions on which customer data was retained and from which customer data was improperly accessed were located in Framingham, Massachusetts.

101. Plaintiff Banks are financial institutions engaged in trade or commerce.

102. TJX's false representations to Plaintiffs regarding its compliance with the Card Operating Regulations and its actions in retaining, failing to safeguard and allowing access to confidential customer data constitute deceptive acts and unfair trade practices within the meaning of Mass. Gen. Laws c. 93A §11. TJX's actions in connection with its failures and misconduct regarding the confidential Visa and MasterCard cardholders' information constitute deceptive acts and unfair trade practices having a direct and substantial effect in Massachusetts causing substantial damages to Plaintiffs and member of the proposed Class.

103. The unfair and deceptive acts and practices described above were knowingly unfair and /or willful, and the Plaintiffs and members of the proposed Class have suffered damages as set forth above.

COUNT THREE
VIOLATION OF THE GRAMM-LEACH-BLILEY ACT AS UNLAWFUL DECEPTIVE ACTS AND PRACTICES UNDER M.G.L. CHAPTER 93A, SECTION 11

104. Plaintiffs incorporate paragraphs 1 through 103 of this Complaint by reference herein.

105. Defendant has a duty pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. and 16 C.F.R. § 313 et seq., not to misuse or inappropriately disclose information received as a third party for the purpose of processing a transaction requested by a customer of its stores.

106. Pursuant to 16 C.F.R. § 313.11(iii), third party recipients of financial data such as Defendant, cannot "use" or "disclose" the information other than in "the ordinary course of business to carry out the activity covered by the exception under which [it] received the information."

107. Defendant was obligated under 16 C.F.R. § 313.11 to only use and disclose customer financial information for the purposes for which it was disclosed, more specifically, to process the transaction.

108. Plaintiff Banks, in the course of business, placed the nonpublic personal information of their cardholder-customers onto the magnetic stripe of their cards with the expectation that retail merchants, such as Defendant, would access that information only for the purpose of processing transactions that are initiated by that customer.

109. Defendant violated the Gramm-Leach-Bliley Act in that it improperly used and disclosed the information in violation of the Privacy Regulations by (i)

maintaining the data well beyond the permitted time-frame; and (ii) allowing the data to be accessed by others for purposes unrelated to the processing of the credit or debit transaction.

110. The above violations constitute unfair and/or deceptive trade practices under Mass. Gen. Laws c. 93A § 11.

111. Plaintiffs and members of the proposed Class have suffered damages as set forth above as a result of these TJX unfair and deceptive trade practices.

112. The unfair and deceptive acts and practices described above were knowingly unfair and /or willful.

COUNT FOUR
NEGLIGENCE

113. Plaintiffs incorporate paragraphs 1 through 112 of this Complaint by reference herein.

114. Defendant owed a duty to Plaintiff Banks to use and exercise reasonable and due care in obtaining and retaining the personal and financial information of Plaintiff Banks and their customers.

115. Defendant owed a duty to Plaintiff Banks to provide adequate security to protect the personal and financial information of Plaintiff Banks and their customers.

116. Defendant breached its duties, allowed an unlawful intrusion into its computer system, failed to protect against such an intrusion; and allowed personal and financial information of Plaintiff Banks and their customers to be accessed by third parties.

117. Defendant knew, or with the reasonable exercise of care should have known, of the risks inherent in retaining such information, and the importance of providing adequate security.

118. As a direct and proximate result of Defendant's carelessness and negligent conduct, Plaintiffs and members of the proposed Class suffered substantial losses as set forth above.

COUNT FIVE
BREACH OF CONTRACT

119. Plaintiffs incorporate paragraphs 1 through 118 of this Complaint by reference herein.

120. TJX had a contract with Fifth Third that required TJX to comply with the Card Operating Regulations.

121. As set forth above, Plaintiff Banks were intended third party beneficiaries to the contract entered into by TJX and Fifth Third.

122. TJX breached its obligations to Plaintiff Banks as third party beneficiaries of TJX's contract with Fifth Third.

123. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and members of the proposed Class suffered losses as set forth above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Banks and members of the proposed Class seek damages against the Defendant for the conduct detailed herein. Plaintiffs demand judgment against Defendant as follows:

1. Certification of the Class under Fed. R. Civ. P. 23 and appointment of Plaintiffs as representatives of the Class and their counsel as lead Class counsel pursuant to Fed. R. Civ. P. 23(g);

2. Money damages;

3. Treble damages for willful and knowing violations of Mass. Gen. Laws c. 93A, § 11;

4. A finding that TJX violated Mass. Gen. Laws c. 93A, §§ 2 and 11 and an order enjoining TJX from any further improper retention of customer data;

5. Reasonable attorneys fees;

6. Costs;

7. Prejudgment interest; and

8. Such other relief as the Court deems equitable and just.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b) Plaintiffs demand a trial by jury on all issues so triable.

Dated May 23, 2007

Respectfully submitted,

/s/ William H. Champlin, III
William H. Champlin, III
William S. Fish, Jr.
Ben A. Solnit
James R. Bryne (BBO #628700)
Tyler Cooper & Alcorn, LLP
CityPlace, 35th Floor
Hartford, Connecticut 06103-3488
Tel: (860) 725-6200

/s/ Joe R. Whatley, Jr.
Joe R. Whatley, Jr.
Richard P. Rouco
Patrick Sheehan (BBO #639320)
WHATLEY DRAKE & KALLAS, LLC
1540 Broadway, 37th Floor
New York, NY 10036
Tel: (212) 447-7070

/s/ Archie Lamb
THE LAMB FIRM, LLC
Archie Lamb
Inge Johnstone
2017 Second Avenue North
Birmingham, Alabama 35203
Tel: (205) 324-4644

/s/ Greg Davis
GREG DAVIS, LLC
Greg Davis
6987 Halcyon Park Drive
Montgomery, Alabama 36117
Tel: (334) 832-9080

/s/ Louis Rutland
RUTLAND LAW FIRM, LLC
Louis Rutland
P.O. Box 551
Union Springs, Alabama 36089
Tel: (334) 738-4770

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated by non-registered participants on May 23, 2007.

S/William S. Fish
William S. Fish

DB00003117V002.doc